ADOA/ISD/ISS
Monthly Cyber Security Tips
NEWSLETTER

SEPTEMBER 2006 Volume 1, Issue 4

Staying Safe on Social Networking Sites

From the Desk of Information Security Services

The popularity of social networking sites continues to increase, especially among teenagers and young adults. The nature of these sites introduces security risks, so you should take certain precautions.

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messenger) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest.

What security implications do these sites present?

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because

- the internet provides a sense of anonymity
- the lack of physical interaction provides a false sense of security
- they tailor the information for their friends to read, forgetting that others may see it
- they want to offer insights to impress potential friends or associates

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information available on them. The more information malicious people have about you, the easier it is for them to take

advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack (see Avoiding Social Engineering and Phishing Attacks for more information). Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal or financial data.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable (e.g., your address, information about your schedule or routine). If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing.
- **Remember that the internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines (see Guidelines for Publishing Information Online for more information).
- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives (see Using Instant Messaging and Chat Rooms Safely for more information). Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, a product of exaggeration, or a joke. Take appropriate precautions, thought, and try to verify the authenticity of any information before taken any action.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam (see Reducing Spam for more information). Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

Children are especially susceptible to the threats that social networking sites present. Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about internet safety, being aware of their online habits, and guiding them to appropriate sites, parents can make sure that the children become safe and responsible users (see Keeping Children Safe Online for more information).

Brought to you by:	
MS-ISAC http://www.msisac.org	US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM